Generation of a watermark being unique to a receiver of a multicast transmission of multimedia

FIELD OF THE INVENTION

The present invention is related to the field of transmission of multimedia to multiple receivers, and more particularly to a method and apparatus for the generation of watermarks being unique to a receiver of a multicast transmission of such media. As used herein, the term "multimedia" can be any type of media such as video, sound etc, typically distributed in the form of a stream of data packets.

BACKGROUND

Multicast transmissions provides efficient one-to-many or many-to-many transmission of multimedia in a distribution network, typically in an Internet environment. A source transmits multimedia in the form of packet data to a group of receivers typically identified by a single IP destination address. Multicast transmissions are well suited for large scale transmissions of multi-media because of scalability; each network link in the distribution network has to transport only one copy of each data packet regardless of the number of receivers.

Authentication and confidentiality can be solved by means of encryption of the data; however, there is still a problem with receivers that retransmit unencrypted data to other receivers. Basic encryption is not sufficient to protect information. One way to detect whom the illegal copy originated from is fingerprinting, i. e embedding unique information, typically a watermark, into each copy of the original data that identifies the receiver receiving the copy.

In unicast transmissions, the number of copies required is multiplied with the number of receivers, which of course implies drawbacks for large scale transmissions. However, it is easy to trace from whom an illegal copy originated, since slightly different copies can be transmitted to each receiver.

In "Large Scale Distributed Watermarking of multicast media through encryption", Parvianninen Roland, Parnes Peter, Department of Computer Science/Centre for Distance Spanning Technology, 2001, it is disclosed a method in which each receiver of a multicast session receives a stream of data having a different unique watermark, while still

retaining the scalability of a multicast transmission. The watermarked streams can be used to trace receivers who make unauthorized copies of the stream. However, this document does not disclose how to provide additional information in the stream of data, which is required for instance to comply with digital right management rules (DRM). The implementation of additional information must fulfill a number of basic requirements such as not significantly affecting the perceptual quality of an image, a video sequence or a sound; it must also be robust to transformations and/or operations that can be applied to the image, video sequence or sound such as color transformation, geometric transformation, translation or rotation, data compression such as JPEG/MPEG, noise, D/A, A/D conversions, image smoothing etc.

SUMMARY OF THE INVENTION

An object of the invention is to provide a method for the generation of watermarks being unique to a receiver of a multicast transmission of multimedia, which also provide additional information, for instance to comply with DRM rules, without creating significant visible and/or audible artefacts in the media.

According to the present invention this is realized in a method of generating a watermark being unique to a receiver of a multi-cast transmission of multimedia data in the form of data packets, comprising a multimedia stream with a multi-bit capacity in a single layer for storing additional information. The principal advantage is that with one single layer of watermarks both global information such as copyright information and user specific information can be embedded with minimum signal degradation. In this way, embedding of multiple watermarks typically in multiple layers can be avoided. This is of importance, since embedding watermarks for instance by stacking them onto each other is a potential source for introduction of perceptible artefacts in the content of the media.

In non-multicast environments a different solution may be used by simply allocating a portion of the watermarks bits for the additional information and a portion of the bits for user specific information typically fingerprint information. However, since the invention finds application in multicast environments such a solution will not be further discussed in this document.

The present invention also provides apparatus and system for performing the method disclosed above.

In a first aspect of some preferred embodiments thereof, the invention provides an efficient method for combining fingerprint- and copyright watermarks by means of one single watermark algorithm in a multicast environment. In another aspect of the

invention, also more watermarks may be deployed. For example, different data packets may be embedded with watermarks from different algorithms. This is still a single-layer watermark, but with different watermark algorithms.

In a second aspect of some preferred embodiments thereof, the invention provides a copy of each data packet to which a receiver has access determined by a sequence of random encryption keys which are sent prior to transmitting.

In a third aspect of some embodiments thereof, the invention provides more than two copies of each data packet.

There is provided, in accordance with a preferred embodiment of the invention, a method of generating a watermark being unique to a receiver of a multicast transmission of multimedia data in the form of data packets, said method comprising the following steps:

-transmitting from a source at least two different copies of each data packet having different watermarks, at least a first watermark and a second watermark, respectively,

-encrypting said copies differently, preferably by means of different encryption keys,

-providing each receiver access to only one of said two copies, thereby providing each receiver with an unique resulting data stream comprising data packets having first and second watermarks, wherein the order in which the first and second watermarks are present in the resulting stream provides the unique watermark,

-providing the data stream with a multi-bit capacity in a single layer for storing additional information.

Preferably, the additional information is global information such as copyright information, producer information and owner information.

Preferably, the source and the receivers are linked together by means of a distribution network such as the Internet.

In a fourth aspect of some preferred embodiments thereof, the invention provides source and receivers linked together by a distribution network based on radio, typically a mobile telephone network such as a GPRS-network, or 3-G network.

There is further provided, in accordance with a preferred embodiment of the invention, a source for transmitting multimedia data to receivers of a multi-cast transmission, said source comprising operational means further comprising or being connectable to transmitting and encryption means which together:

-read data packet i,

-create two watermarked copies $V_0[i]$, $V_1[i]$ of data packet i,

-get two encryption keys SK[2i-1] and SK[2i],

-encrypt the watermarked copies of data packet i $C_0[i]=E(V_0[i]$, SK[2i-1] and $C_1[i]=E(V_1[i]$, SK[2i]),

-add additional information, typically global information such as copyright using the data packets,

-transmit $C_0[i]$ and $C_1[i]$ together with i, where i=1, 2,...,k,

via a network to the receivers.

By means of this method, fingerprint- and global watermarks can be provided using one single watermark algorithm, or multiple watermarks algorithms may be used while still embedding a single-layer watermark.

In a fifth aspect of some preferred embodiments thereof, the invention provides the operational means, transmitting means and encryption means implemented as software.

There is further provided, in accordance with a preferred embodiment of the invention, a receiver for receiving multimedia data comprising receiving and decrypting means, which together:

-receive two packets: $C_0[i]$ and $C_1[i]$,

-get the decryption key for packet i: RKr[i],

-try to decrypt both packets with key RKr[i],

-receive global information,

whereby only one packet will decrypt into a proper data packet: $Vji[i]=D(Cj[i], RKr[i])$, ji ε {0, 1}

-decode and render Vji[i].

According to another preferred embodiment of the invention, the receiving means are arranged to receive more than two data packets and/or the decrypting means are arranged to decrypt more than two data packets.

There is further provided, in accordance with a preferred embodiment of the invention, a system comprising a source, receivers and an intervening distribution network for realizing a method of generating a watermark being unique to a receiver of a multicast transmission of multimedia data in the form of data packets, said method comprising the following steps:

-transmitting from a source at least two different copies of each data packet having different watermarks, at least a first watermark and a second watermark, respectively,

-encrypting said copies differently, preferably by means of different encryption keys,

-providing each receiver access to only one of said two copies, thereby providing each receiver with an unique resulting data stream comprising data packets having first and second watermarks, wherein the order in which the first and second watermarks are present in the resulting stream provides the unique watermark,

-providing the data stream with a multi-bit capacity in a single layer for storing additional information.

A fingerprinted media data stream may decrease illegal copying of the media content, since the origin or the buyer of the media stream can be identified. This can be the only option for pure software solutions where tamper resistant hardware is impossible to implement.

A principal aspect of the invention is to provide one single watermark that provides both identifiers for tracking and comprises additional information. This and other aspects of the invention will be apparent from and elucidated with reference to the embodiments(s) described hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic representation of a system according to a preferred embodiment of the invention.

FIG. 2 illustrates an example of a media stream of data packets transmitted from the source.

Fig. 3 illustrates an example of a fingerprinted media stream transmittable from a receiver of a multimedia multicast transmission.

DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. 1 shows a system for IP multicasting comprising a source 1, for instance a server, and receivers R_1, R_2,...R_n, for instance clients, of which only three are shown. The number of receivers are typically more than 100 000 in a typical Internet multicast environment but is by no means limited thereto. The source 1 and the receivers R_1, R_2,...R_n are linked together by means of a distribution network 2 such as the Internet. Other types of networks are of course also possible, but will not be further disclosed in conjunction to this embodiment.

The source 1 has to access k data packets: P[1], P[2],...P[k] and an encryption algorithm E provided in operational means 10 further comprising or connectable to transmitting and encryption means 20 such that a cover object P=D(E(P, K), K). That is, E(P,

K) encrypts the k:th data packet P[k] with an encryption/decryption key bank k and D(P, K) by means of decryption means 30 decrypts the cover object P. A watermarking algorithm W: P_w=W(P, w), w=U(P_w) and at least two different watermarks, a first watermark w_0 and a second watermark w_1 (illustrated in FIG. 2) are also required. The number of watermarks is not limited to two but can be any suitable number. However, herein only two watermarks are described because of simplicity. Furthermore, the watermarks do not have to be constant and according to a preferred embodiment of the invention, the watermarks can change with time as long as they are not identical, and the source keeps track of them.

The source 1 sends at least two different copies $V_0[i]$, $V_1[i]$ of each data packet P[1], P[2],...P[k], each having a different watermark w_0, w_1. Both copies $V_0[i]$, $V_1[i]$ of the data packets P[1], P[2],...P[k] are encrypted with two different, random encryption keys SK[1], SK[2],...,SK[2k]. The encrypted data packets are then sent to all receivers R_1, R_2,...R_n by means of multicast transmission via a distribution network 2, preferably in an Internet environment hereinafter called "IP multicast". Any given receiver R_1, R_2,...,R_k has access to only one of the encryption keys of one data packet.

The watermarking algorithm W embeds the watermark w in the cover object P, and an detection algorithm U extracts the watermark (w) from the marked object P. A detection algorithm that detects if the watermark (w) is still present can be used instead: U(Pw, w)=B, B ε {true, false}. The source needs 2k random encryption keys, SK[1], SK[2],...,SK[2k] to be able to transmit the data packets of the media stream. A receiver R_1, R_2,...R_n has access to k of these keys SK[1], SK[2],...,SK[2k]: either a receiver key RK_r is RK_r[i]=SK[2i-1] or RK_r[i]=SK[2i], i={1, 2,...,k}.

In Fig. 1, the transmission of encryption keys is not showed in detail. Different strategies may be deployed for this. For instance, keys may be transmitted via the Internet if a channel can be authenticated.

To transmit data packet k, according to a preferred embodiment of the invention, the source 1 performs the following method steps:

-read data packet i P[i],

-create two watermarked copies $V_0[i]$, $V_1[i]$ of data packet i,

-get two encryption keys SK[2i-1] and SK[2i],

-encrypt the watermarked copies $V_0[i]$, $V_1[i]$ of data packet i $C_0[i]$=E($V_0[i]$, SK[2i-1] and $C_1[i]$=E(V1[i], SK[2i]),

-add additional global information such as copyright using the data packets

-transmit $C_0[i]$ and $C_1[i]$ together with i.

FIG. 2 illustrates an example of a media stream of data packets transmitted from the source. A first packet P[1] and a k:th packet P[k] are shown to illustrate how each packet comprises two different encrypted packets $V_0[i]$, $V_1[i]$, which are provided with two different watermarks w_0 and w_1, respectively.

Now is again referred to FIG. 1.

At the receiver side, according to a preferred embodiment of the invention, each receiver R_1, R_2,...R_k receives both packets and tries to decrypt them in the following way by means of the method steps:

-receive two packets: $C_0[i]$ and $C_1[i]$,

-get the decryption key for packet i: RKr[i],

-try to decrypt both packets with the decryption key RKr[i],

-receive global information,

, whereby only one packet will decrypt into a proper data packet: Vji[i]=D(Cj[i], RKr[i]), ji ε {0, 1},

-decode and render Vji[i].

For each data packet the receiver will be able to decode exactly one of the watermarked packets. Which of the two packets is decided by the keys the source has assigned to the receiver.

Fig. 3 illustrates an example of a fingerprinted media stream S transmittable from a receiver of a multimedia multicast transmission. The media streams comprise data packets having different watermarks. A stream from a first receiver R_1 does not correspond to a stream from another receiver. Therefore, each receiver will have his own fingerprinted resulting stream.

If the keys a receiver have access to is unique among all receivers and known by the source, a unique identity string for that user can be defined:

Idr=Br[1], Br[2],...Br[k], Br[i] ε (0, 1).

The identity string can be derived by the source from both keys given to the receiver and the resulting stream from the receiver. From the keys the source sent to the receiver:

Br[i]=0 if RKr[i]=SK[2i-1]

Br[i]=1, if RKr[i]=SK[2i]

From the resulting stream for the user:

Br[i]=0, if U(Vji)=w_0

Br[i]=1, if U(Vji)=w_1

Br[i]=undefined, if neither $C_0[i]$ nor $C_1[i]$ was received or decrypted

If the receiver does not receive all packets, due to for example packet loss or that the receiver tuned in late, the identity strings will not match completely. If n is large enough, the partial identity string will be long enough to be unique among all receivers although some bits are undefined.

Since two copies have to be sent for each data packet, the bandwidth usage has to be doubled for the source and the receivers. Preferably, the bandwidth can be reduced by optimizations. Other demands arise of course, if more than two copies are sent, which is within the scope of the invention.

At any given time, only one of two watermarked packets is actually useful for a single receiver since the other packet cannot be decrypted. If two copies were sent on different multicast groups the receivers can hop between the groups by joining and leaving them as the group the correct packet is transmitted on changes. In this approach it is not only necessary to send the keys to each receiver but also which stream to receive; in such a case one extra bit for each key is required. Also this is within the scope of the invention, but will not be further disclosed, since unfortunately, the join/leave latency for IP multicast transmission is currently too large for this approach. Also, if more than one receiver is on the same network segment most saving is lost.

An alternative way of watermarking could be to watermark one (1) in every x packet, thus reducing the bandwidth requirement to (1+1/x) times the bandwidth of the original stream. Unfortunately, a malicious receiver could remove these watermarked packets and retransmit the resulting degraded stream if x is large. It is therefore necessary to be sure that the degradation is large enough to discourage removal of watermarked packets. One example of this is to only watermark to the I frames of an MPEG video stream or only watermark the last ten minutes of a movie. Also this is within the scope of the invention.

The receiver can be treated as long a term key distributed by out-of-band means when the users registers, either as a downloadable file, preferably protected by SSL/TLS or delivered to the user on a floppy or cdrom. All these solutions have problems when revocation of access is considered. The keys can also be continuously streamed to the users, which is within the scope of the invention.

The amount of keys that each receiver requires depends on the required security. The total size of the keys for one receiver is then keys*keysize. A cryptographic secure random number generator can also generate the bitmasks instead to further reduce storage needs at the source.

Preferably, the key is a 56 bit key, since an attacker has to break a sufficient amount of keys to get enough packets to create an unidentifiable watermarked stream. Any other suitable number of bits is of course evident for a person skilled in the art to use without departing from the invention. Preferably, the keys are generated prior to transmission by the source and stored in files.

It is assumed that it is not possible to either remove the watermark or break the encryption in a reasonable time. It is also assumed that the attacker cannot steal the non-watermarked stream from the source by breaking into the server. If the encryption algorithm is broken an attacker can choose the final watermarked stream and make traitor tracing impossible, but if the encryption algorithm is chosen with care and with large enough key size and the keys are generated properly this can be avoided. The problem of revoking access for a receiver is not considered; however this would require new keys to be transmitted.

If a large enough number of receivers collaborate, p, at least k/p of the original bits from one of the streams will always remain. This can be solved, but is not discussed in this document, since it is well described in prior art.

The invention can for instance be implemented in an existing Java application system for audio transmission over multicast using MPEG-1 audio compression standard. Preferably, "Blowfish" is chosen as encryption algorithm.

No active network elements are required or tamper-resistant smart-cards. The watermarks that make up the fingerprints are not fixed to a certain number of bits or restricted in format, but can be any format the watermarking algorithm requires for robustness. To avoid attacks it is also possible to increase the number of watermarks in one media stream.

As used in the following claims, the words "comprise" or "include" or their conjunctions means "including, but not necessarily limited to.